



HM Prison &
Probation Service

Code of Practice

Electronic Monitoring Data

February 2018

Code of Practice

Electronic Monitoring Data

Electronic Monitoring Directorate

February 2018

Printed on paper containing 75% recycled fibre content minimum.

Printed in the UK by the Williams Lea Group on behalf of the Controller of Her Majesty's Stationery Office



Contents

Purpose.....	2
Legal Framework.....	3
Imposing and Electronic Monitoring Requirement or Condition.....	4
The Data and Monitoring the Requirement / Condition.....	4
Sharing Information.....	6
Transmitting Data.....	9
Data Compromise or Loss.....	9
Data Rectification and Erasure.....	10
Holding and Retaining Data.....	11
Data Protection and Processing Roles.....	11
Home Detention Curfew.....	14
Single Requirement Electronic Monitoring Orders.....	15

PURPOSE

1. On a date to be confirmed in 2019, the Ministry of Justice (MoJ) will commence a new electronic monitoring service which will include curfew and/or location monitoring of subjects who have had such a requirement or condition imposed through a Court Order or a prison licence.
2. To allow for the location monitoring of an offender to take place, where it is not ancillary to another requirement and where it is imposed as part of a community sentence (community order or suspended sentence order), legislation creating the power for freestanding monitoring needs to be brought into force. When commencing this power, in accordance with the provisions of the Criminal Justice Act 2003 ¹(as amended by the Crime and Courts Act 2013), the Secretary of State is required to issue a Code of Practice relating to the processing of personal data in the course of electronic monitoring of persons serving a community sentence with an electronic monitoring requirement.
3. In addition, the provisions of the Criminal Justice and Courts Services Act 2000², require the Secretary of State to issue a Code of Practice relating to the processing of data gathered in the course of electronic monitoring of persons with an electronic monitoring condition as part of a prison licence.
4. The issuing of this Code of Practice fulfils both requirements (as set out in paragraphs 2 and 3 above) so far as the processing of electronic monitoring data concerns the new electronic monitoring service. It clarifies the expectations, safeguards and broad responsibilities for the collection, retention, processing and sharing of electronic monitoring data. It has been drafted in consultation with MoJ colleagues and stakeholders including:
 - The Information Commissioner’s Office;
 - The Investigatory Powers Commissioner’s Office;
 - The Police;
 - The Youth Justice Board; and
 - Those responsible for managing the performance against contract of Community Rehabilitation Companies (CRCs).
 - The Parole Board
5. In accordance with the legislative requirements for this Code, its contents are not legally binding on any party. It is provided to help Data Controllers and Data Processors involved in electronic monitoring of persons subject to relevant orders/licences to understand the legal framework and adopt good practice. Its content does not seek to remove or replace any of the contractual provisions that are in place for CRCs.

¹ Section 215A

² Section 62B (as inserted by the Criminal Justice and Courts Act 2015)

6. As the new electronic monitoring service will not go live until 2019, this Code has been written to accord with the provisions of the Data Protection Bill (specifically Part 3) which is currently before Parliament. Its content will be reviewed after the Bill becomes law (expected mid 2018) to ensure it aligns with the new data protection legislation.

THE LEGAL FRAMEWORK

7. The legal framework for electronic monitoring of the orders/licences in scope of this document is set out in the Criminal Justice and Court Services Act 2000, the Criminal Justice Act 2003, the Offender Management Act 2007, the Crime and Courts Act 2013 and Criminal Justice and Courts Act 2015.
8. The electronic monitoring information that will be processed constitutes both personal data and sensitive personal data as defined in data protection legislation. Therefore, unless an exemption applies, the processing of it must comply with the six data protection principles set out below:
 - Fairly and lawfully processed, in a transparent manner;
 - Processed for specified, explicit, and legitimate purposes and not processed in a manner that is incompatible with those purposes;
 - Adequate, relevant and limited to what is necessary;
 - Accurate and up to date;
 - Not kept for longer than is necessary;
 - Held securely, including being protected against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;
9. The processing of electronic monitoring data referred to in this document is for law enforcement purposes, specifically the prevention of crime, execution of criminal penalties and safeguarding against the prevention of threats to public security. Where necessary and proportionate to do so, information may be shared with relevant Agencies for other law enforcement purposes such as, investigation, detection or prosecution of criminal offences. Further information on data sharing is set out in paragraphs 25 to 36
10. It is recognised that the processing of personal and sensitive personal information engages Article 8 of the European Convention of Human Rights i.e. the right to respect for private and family life. However, Article 8 is not an absolute right and public authorities are permitted to interfere with it if it is lawful and proportionate to do so.
11. The Ministry of Justice considers that it is both lawful and proportionate to process the data referred to in this document for the purposes of complying with relevant electronic monitoring orders/licences issued under the legislation referred to in paragraph 7 above. Personal data will only be shared if it is justified and proportionate where it is lawfully permitted, and processing shall be

in compliance with the provisions of data protection legislation for law enforcement purposes, as referred to in paragraph 9 above.

IMPOSING AN ELECTRONIC MONITORING REQUIREMENT OR CONDITION

12. It is a decision for the Courts whether to impose an electronic monitoring requirement as part of a Court Order and it is incumbent upon them to consider any statutory safeguards and issues of fairness and proportionality.
13. An electronic monitoring condition can be imposed on a prison licence administratively by the Parole Board or by the governor/director of a prison on behalf of the Secretary of State when a subject is released from prison. Prison governors/directors will only set licence conditions in consultation with probation providers. In accordance with Her Majesty's Prison and Probation Service (HMPPS) policy, the aims of the licence period are to protect the public, to prevent re-offending and to secure the successful re-integration of the offender into the community. Licence conditions should be preventative as opposed to punitive and must be proportionate, reasonable and necessary. However, the mandatory curfew imposed under the home determination curfew (HDC) is also punitive in that it reflects the fact that the prisoner is still serving the custodial element of the sentence.
14. For determinate sentenced offenders, the National Probation Service (NPS) has the authority to add, remove and amend licence conditions where it is necessary and proportionate to do so. Any bespoke conditions (i.e. not a licence condition identified in the policy) must first be approved by the Public Protection Casework Section (PPCS) in the MoJ. PPCS may also vary an indeterminate sentenced offender's licence conditions where it is necessary and proportionate to do so and licence conditions for subjects managed by CRCs.

THE DATA AND MONITORING THE REQUIREMENT / CONDITION

15. The MoJ has contracted with four suppliers on a Lot basis to enable the monitoring of an electronic monitoring requirement/condition.
16. Lot 1 is for an Electronic Monitoring Service (EMS). EMS will install/remove the necessary equipment, monitor the subject's compliance with the electronic monitoring requirements/conditions and report breaches to the appropriate organisation. EMS also has specific responsibilities for single requirement electronic monitoring orders and Home Detention Curfew cases (see paragraphs 62 to 66 for further details). EMS will collect and process subjects' personal data.

17. The other three contractors will not have access to personal data and will provide the following services:

- Lot 2 - mapping of data from the tags and the application of business logic to determine their location. The location data is related to a tag reference and not a person. The company that provides this service will not have any access to Lot 1 data i.e. the subject's personal data (see paragraph 24 below);
- Lot 3 - the provision of electronic monitoring tags;
- Lot 4 - the provision of a resilient mobile communications network to enable transmission of voice and data relating to the monitoring of subjects.

18. The data processed by EMS will be that which is necessary to:

- Ensure the right subject is tagged;
- Monitor subjects' compliance with, and to enforce, the relevant orders/licences.
- Where appropriate, monitor subjects' location;
- Ensure that EMS is able to discharge its contractual obligations and to allow for the monitoring of its performance against contractual requirements;
- Safeguard the public and staff e.g. recording notes of any threatening or violent behaviour by the subject or others at the premises and sharing this information where appropriate;
- Assist Criminal Justice Agencies with criminal enquiries. The circumstances in which such data will be shared are set out in the body of this document;
- Assist the MoJ in meeting its obligations under the Equality Act 2010.

19. EMS will only collect and retain the personal and sensitive personal data necessary to meet its contractual obligations. The data will only be processed in accordance with data protection legislation. Unless an exemption within the relevant Act applies, or other legislation permits, the data will only be processed for the purposes set out in paragraph 9. Security and access to data are restricted in accordance with legislation and guidance. Only the necessary amount of personal and sensitive personal data will be shared for the purposes of meeting the requirements set out above.

Location and Curfew Monitoring

20. Where the relevant order/licence includes a location monitoring requirement/condition (other than curfew), the subject will be fitted with a location monitoring enabled tag. The location monitoring hardware and associated software will capture the subject's location 24 hours a day in compliance with the

order/licence. However, where location monitoring is only imposed to monitor a specific requirement/condition, such as an exclusion zone, active monitoring of the location data will only take place if there is a breach of that requirement/condition. It will not be actively monitored at other times. This will be explained to the subject as part of a Fair Processing Notice (see paragraph 25). The remaining location data will not be utilised unless or until there is a lawful reason to do so.

21. If the subject has been given a standalone location monitoring requirement (location monitoring that is not ancillary to another requirement) all the location data captured may be monitored.
22. Curfew requirements will be monitored through radio frequency (RF) technology. In cases where the subject has both a location monitoring requirement and a curfew, they will be fitted with a location monitoring enabled tag which will switch to RF to monitor the curfew. In cases where subjects are given a curfew but not a location monitoring requirement they will be fitted with an RF only enabled tag. However, the movements of a subject fitted with an RF tag may be captured if and when the individual passes a location where another monitoring device has been installed as it will read the presence of RF tags within the immediate vicinity.
23. Decision makers will be made aware of the location data that will/may be captured and should consider this when determining whether it is necessary and proportionate to impose an electronic monitoring requirement.
24. The location data held by Lot 2 will only be sent to Lot 1 and linked with the subject's personal details if there is a legitimate and lawful reason to combine the two data sets. For example, if the subject has a standalone location monitoring requirement, if there is a breach of an exclusion zone or to assist law enforcement agencies such as the Police, to investigate, prevent or detect crime. The circumstances in which this data and all other electronic monitoring data will be shared are set out in paragraphs 25 to 36.

SHARING INFORMATION

25. All electronic monitoring subjects will, on induction, receive a Fair Processing Notice, which will meet the requirements bestowed upon data controllers by data protection legislation and explain how the data collected against them will be used by EMS, and will explain the data subject's rights. The wording of this notice will include a statement to the effect that the system may capture the subject's location throughout the day and, where necessary and proportionate to do so, this data may be shared with others for law enforcement purposes.
26. Personal data must only be shared where it is permitted by law and is justified, necessary and proportionate to do so. It is the responsibility of the Data Controllers

identified later in this document, to ensure that this is enforced in respect of personal data for which they are accountable.

27. There are express powers within the Offender Management Act 2007 that allow for the sharing of offender information by specific parties for specific purposes. Section 14(4) of the Offender Management Act 2007 provides that the sharing of information is permitted where it is necessary or expedient for the following purposes:

- probation purposes;
- the performance of functions relating to prisons and prisoners;
- any other purposes connected with the management of offenders (including the development or assessment of policies relating to matters connected with the management of offenders).

28. There are also common law powers which enable the sharing of information between parties.

29. The Crime and Disorder Act 1998 (as amended by the Police and Justice Act 2006 and the Policing and Crime Act 2009) and the Crime and Disorder (Overview and Scrutiny) Regulations 2009 also provide powers to share information in order to meet the provisions of that Act.

30. Stakeholders appointed to supervise/enforce the orders/licences will have access to electronic monitoring data on the EMS system via secure email and an electronic Portal, captured on those orders for the purposes for which it was obtained (see paragraph 8). So, for example:

- The MoJ, will have access to all records and reports for the purposes of monitoring compliance with the contract;
- The National Probation Service (NPS) will have access to electronic monitoring data gathered on Orders/licences where they act as the Responsible Officer for that subject on that particular Order/licence (including those that are in the process of being allocated by NPS to a CRC), or if they are required to take enforcement action against a subject.
- Prisons will be able to submit electronic monitoring notifications onto the Portal;
- PPCS will have access to records on offenders released on licence from prison custody and will routinely pass information onto the Parole Board as evidence for recall to custody or to inform release decisions;
- The MOJ HDC Appeals Team will have access to records on offenders recalled to prison from release on HDC, and will occasionally pass information onto contracted forensic experts in order to determine the cause of damage to the EM equipment;
- Her Majesty's Courts and Tribunals Service (HMCTS) will be able to submit electronic monitoring notifications to EMS, view them on the Portal and alert EMS to any necessary amendments;
- Community Rehabilitation Companies (CRCs) will have access to data gathered on Orders/licences where they act as the Responsible Officer for that subject on that particular Order/licence.

- Youth Offending Teams (YOTs) will have access to data gathered on Orders/licences where the Team acts as the Responsible Officer for that subject on that particular Order/licence, or if they are required to take enforcement action against a subject.
 - Where it is proportionate and necessary, Police Forces will be given data to assist with the investigation, prevention and detection of crime. They may also be given data to assist with assessing risk and managing compliance of subjects such as prolific offenders and those subject to Multi Agency Public Protection Arrangements. Data may also be shared to assist in the apprehension of a subject following a breach of their electronic monitoring condition. Further details of the data share with the Police will be set out in Data Sharing Agreements with each Force.
31. Where requested, if necessary and proportionate, subject data may be shared with those organisations without the subject's consent and other public authorities for other law enforcement purposes such as for the detection and prevention of crime, in accordance with data protection legislation.
32. Information may also be released to a wider range of requestors e.g. a solicitor acting on behalf of the subject, if the subject provides their consent.
33. Information will only be released if lawful and in accordance with data protection legislation unless otherwise directed by a Court. Any information disclosed must only be used for the purpose(s) that led to its disclosure and it must not be further processed or passed on in a manner that would be incompatible with that purpose(s).
34. EMS will not have direct access to information held on stakeholder systems, but relevant information will be shared via secure email or the Portal to enable EMS to fulfil its contractual obligations.
35. Stakeholders and EMS may also pass information to one another where there is a lawful basis to do so. This includes sharing information relating to the risk the subject may pose to others where it is necessary and relevant to the protection of staff and the public. Information may also be shared for safeguarding purposes or to report potential criminal behaviour.

Subject Access Requests

36. Individuals who are subject to electronic monitoring conditions or requirements are entitled to ask for a copy of the personal information held on them by writing to EMS. The relevant contact details for such requests will be explained as part of their electronic monitoring induction.

Freedom of Information Requests

37. All data controllers in this process are subject to the provisions of Freedom of Information Act 2000 and shall assist and co-operate to enable each other to comply with their respective statutory duties in relation to requests for Information. Any requests for information in relation to the electronic monitoring service should be submitted to the following email address:

data.access@justice.gov.uk.

TRANSMITTING DATA

38. Data transferred from tags to the monitoring centre will be encrypted. All data shared by EMS with stakeholders will be via secure email or the electronic monitoring portal. Data transmitted to the portal will be encrypted. In addition, supervising/enforcing organisations may receive an alert via SMS from EMS to look at their email or the portal.
39. All communications with stakeholders must accord to the Government Security Classification tier for the data being shared which will usually be 'Official' including some that may be marked Official Sensitive. Parties carrying out the functions outlined in this Code should make themselves aware of, and adhere to, their organisation's information security policies and procedures in regards to handling data in a manner appropriate for the assigned security classification.
40. All staff have a duty of confidentiality and a personal responsibility to safeguard any information with which they are entrusted. This includes ensuring that they comply with the legal and regulatory requirements and standards, for example the encryption of personal data on removable media

DATA COMPROMISE OR LOSS

41. Legislation and regulation requires stakeholders to appropriately handle and protect information. Those same demands also require stakeholders to report, manage, and in some cases escalate, all events where information requiring protection is either lost or compromised. Every staff member, irrespective of role, grade, or location, is required to report an event involving loss or compromise of data.
42. 'Lost' is defined as information where the location is unknown (this can be both internally and externally) or where its suspected location is out of the stakeholder's control.

43. 'Compromise' is defined as information that has been subject to unauthorised access, use, or modification.
44. All stakeholders must follow their local policies on reporting a compromise or loss of data. In addition, where this concerns shared MoJ data, the stakeholder must inform the MoJ as soon as possible, or no later than 24 hours after the compromise / loss is identified.
45. On being notified of the possible incident, the controller must establish whether it is a potential significant incident. Some of the factors to consider include:
 - the nature of the information (is it personal information or sensitive corporate information?)
 - the number of individual records involved (if personal information)
 - the possible impact of the incident, including the apparent risk to the individuals, their families (for instance, children), staff, victims, offenders under supervision, members of the public and MoJ's operations or reputation;
46. If a personal data breach is likely to result in a risk to the rights and freedoms of individuals, the data controller responsible for the data must notify the breach to the Information Commissioner, without undue delay, and where feasible, not later than 72 hours after becoming aware of it.
47. If the incident is considered serious or impacting, the lead manager must immediately inform the appropriate Senior Official through the management line. All contracted providers should report the incident through the contractual line (designated contract manager). An investigation should take place into the circumstances of the breach to ensure that lessons are learned and shared where necessary.

DATA RECTIFICATION AND ERASURE

48. Should stakeholders become aware that a subject's personal data is inaccurate or incomplete, they must take reasonable steps to rectify the situation.
49. Stakeholders must, without undue delay, erase personal data where its processing would infringe the principles set out in paragraph 8 above, unless the data is required as evidence.
50. If the subject requests rectification or erasure of their personal data, then the relevant party must respond to the subject informing them of the outcome of their request. Should the request be refused the subject must be informed of their right to take the matter up with the Information Commissioner and/or the Court.

HOLDING AND RETAINING DATA

Holding Data

51. All stakeholders must hold the data securely in accordance with relevant policies or detailed technical specifications within relevant contracts. These provisions must accord with Cabinet Office security standards and the Data Protection Bill.
52. All stakeholders must ensure the integrity and confidentiality of the information they hold. All staff that have access to the information must be suitably trained, be security cleared at the appropriate level for the information that they handle and comply with the Official Secrets Act 1989. Access to the data must only be by those who have a legitimate need to review the data. Inappropriately accessing the data without the data controller's knowledge may constitute a criminal offence.
53. Data must not be held outside of the European Economic Area.

Retaining Data

54. All parties carrying out the functions set out in this Code of Practice must adhere to their organisation's record management policies and procedures specifically in relation to retention and destruction of data. Such policies and procedures must be compliant with data protection legislation. Personal data must not be held for longer than is necessary.
55. EMS will hold electronic monitoring subject data for up to 6 years post order end unless otherwise directed by the MoJ. Thereafter it will be securely destroyed. The retention policy will be reviewed every two years to determine whether there is sufficient evidence to warrant a threshold of less than 6 years.

DATA PROTECTION AND PROCESSING ROLES

56. A **Data Controller** is a competent authority (as defined by the Data Protection Bill) that, either alone or jointly, determines the purposes for which, and the means by which, any personal data are, or are to be processed. It is the Data Controller that must exercise control over the processing and carry data protection responsibility for it.
57. A **Data Processor** in relation to personal data, is any person (other than an employee of the Data Controller) who processes the data on behalf of the Data Controller. **Processing**, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:
- collection, recording, organisation, structuring or storage,
 - adaptation or alteration,

- retrieval, consultation or use,
- disclosure by transmission, dissemination or otherwise making available,
- alignment or combination, or
- restriction, erasure or destruction.

58. The Data Controllers of electronic monitoring information are listed below:

MoJ

The MoJ, as it is the Authority that contracts EMS to deliver an electronic monitoring service. It determines the purposes for which data are processed for electronic monitoring of subjects on community sentences and prison licence, including Home Detention Curfew (HDC). Further information on HDC is set out in paragraphs 62-65 below.

Officials in the MOJ have responsibility for considering, on behalf of the Secretary of State, any appeals against recall to custody for breach of the electronically monitored requirements of the licence. The MoJ is the parent Department of HMCTS and HMPPS (which includes public sector Prisons and the NPS). Briefly, the duties of each of those bodies, so far as it applies to the electronic monitoring requirements on the orders in scope of this Code, include the following:

Public Sector Prisons and HMCTS

Public Sector Prisons and HMCTS will be responsible for issuing notifications of electronic monitoring requirements to EMS on prison licences and Court Orders respectively.

HMPPS HQ

The Electronic Monitoring Directorate in HMPPS HQ is responsible for monitoring EMS' compliance with the contract. PPCS is responsible for revoking prison licences, including HDC, following a breach of conditions, and issuing recalls to custody. PPCS can also vary licence conditions as explained above.

NPS

Save for the curfew element of HDC and single requirement electronic monitoring Orders (see paragraph 62 -66 below), NPS is responsible for supervising the following categories of offenders in the community:

- those it has assessed as posing a high or very high risk of serious harm or serious recidivism to the public (both those sentenced to community orders or suspended sentence orders and those released from custody on licence or at the end of a short sentence);

- offenders whose cases are automatically subject to the Multi-Agency Public Protection Arrangements (MAPPA), because of the nature of their index offence;
- foreign national offenders who are of interest to the Home Office and may be subject to deportation; and
- a small number of cases retained for public interest reasons.

Should a subject breach the EM requirement (see paragraphs 62 - 66 for caveats) NPS will consider:

- i) issuing a warning letter if the breach is considered unacceptable
- ii) taking breach action by referring the case back to Court for it to amend, cancel, or vary a community sentence. NPS also do this on cases referred to it by CRCs (see below);
- iii) varying a licence condition;
- iv) recommending to PPCS a recall to prison custody of an offender on prison licence.

NPS also has a duty imposed by section 4 of the Offender Management Act 2007 which relates to the giving of assistance to any court in determining the appropriate sentence to pass, or making any other decision, in respect of a person charged with or convicted of an offence.

Private Prisons

Private prisons are Data Controllers that will notify EMS when individuals in their custody are required to be released on licence with an electronic monitoring requirement.

CRCs

CRCs are Data Controllers. Save for the curfew element of HDC and single requirement curfew orders, CRCs are responsible for supervising medium and low risk of serious harm offenders who have an electronic monitoring requirement or condition attached to their community sentence or licence. Should a subject breach the EM requirement (see paragraphs 62-66 for caveats) CRCs will consider:

- i) issuing a warning letter if the breach is considered unacceptable;
- ii) taking breach action by referring the case to the NPS Enforcement Officer for Court action i.e. for it to amend, cancel, or vary a community sentence;
- iii) recommending to PPCS a recall to prison custody of an offender on licence.

The Police

The Police are Data Controllers who may assist in managing compliance. They are responsible for the apprehension of subjects who have breached relevant electronic monitoring orders. In specific circumstances, the Police may also use and interpret electronic monitoring data for the purposes of assessing an offender's risk as part of their multi-agency responsibilities or for the detection or prevention of crime.

YOTS

YOTS are Data Controllers. They are the Responsible Officers for under 18s and may take appropriate action following a breach of an order or licence. Therefore they generally determine the use of the electronic monitoring data for children and young people subject to relevant Orders.

Others

Data may also need to be shared with other Government Departments where it is lawful, proportionate and necessary to do so. Those Departments will be Data Controllers of the information in their possession.

59. Each Data Controller has full data protection responsibility to safeguard any personal information or data to which they have access and to ensure confidentiality. They will be responsible for maintaining control and security of the information within their organisation's systems.
60. The Data Processor of the electronic monitoring personal information will be EMS who collate and disseminate information on behalf of the MoJ.
61. All parties above must ensure that significant decisions affecting subjects are not based solely on automated processing unless that decision is required or authorised by law.

HOME DETENTION CURFEW

Adult Offenders

62. Offenders serving sentences of imprisonment of less than four years who are released early on HDC not only have a curfew but general licence intended to protect the public, to prevent re-offending and to secure the successful re-integration of the offender into the community. The curfew conditions expire at the half way point of the sentence, but general conditions remain in force until the end of the sentence.
63. EMS monitor the curfew conditions and are permitted by reference to terms of the licence to perform the function of a case manager in both authorising absence from curfew address and in issuing warning letters for minor curfew breaches without

recourse to anyone else. All other non-compliance must be reported to PPCS to consider whether a recall to prison custody is necessary.

64. Supervising Officers (CRCs, NPS or YOTs) are responsible for supervising the general licence conditions and for reporting any breaches of those conditions to PPCS.

Under 18s

65. Children and young people (under 18s) serving a sentence of detention under section 91 of the Powers of Criminal Courts (Sentencing) Act 2000 may be released on HDC. In addition, those serving a Detention and Training Order (DTO) may be subject to electronic monitoring during the community element of their DTO. Young people serving DTOs serve the first half in custody, and the second half in the community. Most young people serving a DTO of 8 months or more can be released one or two months earlier (depending on DTO length) than the normal mid-point of sentence. If released early, they will be subject to an electronically monitored curfew requirement for the period that the young person would have otherwise have been in detention (i.e. until the midpoint of the DTO) and general conditions. The curfew condition is monitored by EMS. YOTs are responsible for supervising the general licence conditions. All non-compliance events are reported to the Youth Offending Team (YOT) to consider whether the matter should be taken to Court for enforcement action.

SINGLE REQUIREMENT ELECTRONIC MONITORING ORDERS

66. EMS acts as the Responsible Officer for Single Requirement Electronic Monitoring Orders issued by a Court. Serious violations of those orders are reported to the appropriate body to take enforcement action. For adult Orders this will be the National Probation Service. For Youth Rehabilitation Orders the enforcement body is the Youth Offender Team.

Barcode goes here:

2.93cm (h)

3.74cm (w)

16.2cm to the right of
page

25.1 below page